CLAIMS

What is claimed is:

1. A system comprising:

a plurality of certificate authorities (CAs) in which each CA maintains and distributes digital certificates revoked by itself in the form of a certificate revocation list (CRL), and different CAs may use different CRL distribution mechanisms;

a plurality of CRL databases for storing the consolidated CRLs from multiple CRL retrieval agents and/or the replications of CRLs; and

a CRL access user interface for providing a uniform set of APIs for user's accessing the CRLs CRL databases, said system enabling consolidation and access of the certificate revocation list (CRL).

2. A system according to claim 1, wherein said plurality of CRL databases include a central CRL database and a plurality of CRL replication databases, said central CRL database for storing the consolidated CRLs from the multiple CRL retrieval agents, and said plurality of CRL replication databases for storing the replications of the CRLs of the central CRL database.

3. A system according to claim 1, wherein said plurality of CRL retrieval agents include a LDAP/CRL retrieval agent, for periodically retrieving CRLs from specified LDAP servers and updating the CRL databases.

4. A system according to claim 1, wherein said plurality of CRL retrieval agents include a HTTP/CRL retrieval agent, for periodically retrieving CRLs from specified HTTP servers and updating the CRL database.

5. A system according to claim 1, wherein said plurality of CRL retrieval agents include a RFC1424/CRL retrieval agents, for periodically sending RFC1424/CRL retrieval request and receiving CRL retrieval reply.

6. A system according to claim 1, wherein said plurality of CRL retrieval agents include a Http receiver agent triggered by a HTTP request, said Http receiver agent verifies an authorization of the requester, if successful, said agent stores each transmitted CRL in the CRL databases.

7. A system according to claim 1, wherein said plurality of CRL retrieval agents further verifies the integrity and the authenticity of the retrieved CRLs.

8. A system according to claim 1, wherein a particular replication architecture is used among said plurality of CRL databases in order to maintain database consistency.

9. A system according to claim 2, wherein a sub-and-spoke replication architecture is used among said central CRL database and said plurality of CRL replication databases.

10. A system according to claim 1, wherein said system is also adapted for consolidating and accessing at least one kind of black list.

11. In a secure network implemented by digital certificates, a method for certificate revocation list (CRL) consolidation and access, wherein a plurality of certificate authorities (CAs) maintain and distribute the digital certificates revoked by themselves in the form of CRLs, and different CAs may use different CRL distribution mechanisms, said method comprising the steps of:

creating a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs, for consolidating the CRLs from multiple CAs;

storing the consolidated CRLs from multiple CRL retrieval agents or the replications of CRLs into a plurality of CRL databases; and

accessing the CRLs from the CRL databases by a uniform set of APIs.

12. A method according to claim 11, said plurality of CRL databases include a central CRL database and a plurality of CRL replication database, said central CRL database for storing the consolidated CRLs from multiple CRL retrieval agents and said plurality of CRL replication database for storing the replications of the CRLs of the central database.

13. A method according to claim 11, wherein said method is also adapted for consolidating and accessing all kinds of black lists.

14. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing certificate revocation list (CRL) consolidation and access,, the computer readable program code means in said article

of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 11.

15. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing certificate revocation list (CRL) consolidation and access, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 11.

16. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for certificate revocation list (CRL) consolidation and access, said method steps comprising the steps of claim 11.

17. A method comprising:

employing a secure network implemented by digital certificates for certificate revocation list (CRL) consolidation and access, with a plurality of certificate authorities (CAs) maintaining and distributing the digital certificates revoked by themselves in the form of CRLs, wherein different CAs may use different CRL distribution mechanisms, including the steps of:

creating a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs, for consolidating the CRLs from multiple CAs;

storing the consolidated CRLs from multiple CRL retrieval agents or the replications of CRLs into a plurality of CRL databases; and

accessing the CRLs from the CRL databases by a uniform set of APIs.

19. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for certificate revocation list (CRL) consolidation and access, said method steps comprising the steps of claim 18.

20. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing certificate revocation list (CRL) consolidation and access, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 18.

21. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing certificate revocation list (CRL) consolidation and access, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 18.